User Manual

FSW3208M

8+2 Gigabit Ethernet WebSmart Switch

CTC UNION TECHNOLOGIES CO., LTD.

LEGAL

The information in this publication has been carefully checked and is believed to be entirely accurate at the time of publication. CTC Union Technologies assumes no responsibility, however, for possible errors or omissions, or for any consequences resulting from the use of the information contained herein. CTC Union Technologies reserves the right to make changes in its products or product specifications with the intent to improve function or design at any time and without notice and is not required to update this documentation to reflect such changes.

CTC Union Technologies makes no warranty, representation, or guarantee regarding the suitability of its products for any particular purpose, nor does CTC Union assume any liability arising out of the application or use of any product and specifically disclaims any and all liability, including without limitation any consequential or incidental damages.

CTC Union products are not designed, intended, or authorized for use in systems or applications intended to support or sustain life, or for any other application in which the failure of the product could create a situation where personal injury or death may occur. Should the Buyer purchase or use a CTC Union product for any such unintended or unauthorized application, the Buyer shall indemnify and hold CTC Union Technologies and its officers, employees, subsidiaries, affiliates, and distributors harmless against all claims, costs, damages, expenses, and reasonable attorney fees arising out of, either directly or indirectly, any claim of personal injury or death that may be associated with such unintended or unauthorized use, even if such claim alleges that CTC Union Technologies was negligent regarding the design or manufacture of said product.

TRADEMARKS

Microsoft is a registered trademark of Microsoft Corp.
HyperTerminal™ is a registered trademark of Hilgraeve Inc.

WARNING :

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and if not installed and used in accordance with the instruction manual may cause harmful interference in which case the user will be required to correct the interference at his own expense. NOTICE : (1) The changes or modifications not expressively approved by the party responsible for compliance could void the user's authority to operate the equipment. (2) Shielded interface cables and AC power cord, if any, must be used in order to comply with the emission limits.

CTC Union Technologies Co., Ltd.
Far Eastern Vienna Technology Center (Neihu Technology Park)
8F, No. 60, Zhouzi St.
Neihu, Taipei, 114
Taiwan
Phone : +886-2-2659-1021
FAX : +886-2-2799-1355

FSW3208
8+2 Gigabit Smart Switch
Stand-alone / Rack Type

User Manual
Version 3.4 April 2008 Release

This manual supports the following model :
FSW3208M

This document is the official release manual. Please check CTC Union's website for any updated manual or contact us by E-mail at info@ctcu.com. Please address any comments for improving this manual or to point out omissions or errors to marketing@ctcu.com. Thank you.

TABLE OF CONTENTS

1.0 Introduction 7
1.1 Main Features 7
1.2 Start to Manage This Switch 8
2.0 Web management 9
2.1 Configurations 10
2.1.1.1 System information 10
2.1.1.2 DHCP 11
2.1.1.3 relocate HTTP port number 11
2.1.1.4 Tag VLAN management group (CPU port) 11
2.1.2 Ports 12
2.1.3 Port-based VLAN 13
2.1.4 Tag-based VLAN 13
2.1.4 Tag-based VLAN 14
2.1.5 Port Trunking 17
2.1.6 Port Mirroring 18
2.1.7 Quality of Service 19
2.1.8 Storm Control 21
2.1.9 LACP 21
2.1.9 LACP 22
2.1.10 RSTP 23
2.1.11 IGMP 25
2.1.12 802.1x 26
2.2 Monitoring 26
2.2 Monitoring 27
2.2.1. Port Statistics 27
2.2.2 LACP Status 28
2.2.3 RSTP Status 29
2.2.4 IGMP Status 29
2.2.5 Ping 29
2.2.5 Ping 30
2.3 Maintenance 31
2.3.1 Warm Reboot 31
2.3.2 Factory Default 31
2.3.3 Firmware Update 31
2.3.4 Config File 32
3.0 Terminal Mode Management 32

1.0 Introduction

This web smart switch is a high speed switch that provides up to 8 10/100/1000Mbps copper Ethernet ports, besides, it provides many advanced function for nowadays variety of network application but at lower cost. User doesn't have to learn many sophisticated management function which are usually shown in SNMP switch but just to learn some simple or common control or setting function through either out-of-band RS232 port or Ethernet port, however, some new, advanced and important function such as Tag-VLAN, Trunking, RSTP and IGMP are also supported same as SNMP switch, this means, user doesn't have to pay high cost as tradition layer 2 SNMP switch while he still can get advanced or common function to meet requirement of advanced network application. This makes it very suitable for small or medium size company to build up simple network at beginning phase with lower cost. An optional long-ear accessory also makes it possible to operate in the rack mount environment.

Non-blocking and maximum wire speed performance are designed on all switched ports, it not only supports auto-negotiation but also AUTO-MDIX function on all switched 8 10/100/1000M RJ-45 Gigabit copper ports no matter running with half or full duplex mode, these function make user easy to use and reduce the matching effort between straight and cross-over line issues.

8G web smart switch supports both port-based and 802.1Q (tag-based) VLAN to catch-up the application needed for coming VLAN age. To increase bandwidth application, it supports up to 4 trunk groups with maximum 8 ports on one Trunk, moreover, these trunk ports are with fair-over function to provide redundant back-up when one or some of trunk ports malfunction. Moreover, to reduced convergent time of STP protocol, Rapid STP (RSTP) is supported, to support multicast application IGMP is also supported. ,

Fully LED status display ease user's installation and inspection, a reset button is also provided to make user easy to go back to default setting.

1.1 Main Features

This switch provides the following main features:

- Non-blocking, full-line speed, store-and-forward
- Support jumbo frame, Max. packet length 9600 bytes
- Auto-Negotiation and Auto-MDIX on all 10/100/1000M copper ports
- Up to 8 10/100/1000 RJ-45 copper ports
- 144K byte packet buffer, 8K MAC entries
- Support port-based VLAN and tag-based (802.1Q) VLAN
- Support RSTP, IGMP, DHCP
- Support "relocate port number" to " http operation "
- Port trunk with fail-over capability
- Support flow control for both full/half duplex operations
- Support Multicast storm, Broadcast Storm control as well as Flooding Control
- Support port mirroring
- Support Telnet
- LED display for each port to show link and activity status
- Desktop and optional Rack mountable kit
- Reset to default
- Field-code-upgrade through web browser

1.2 Start to Manage This Switch

Either way user may start to manage this switch, web mode through Ethernet port or terminal mode through RS232 port.

1,2,1 Web mode default setting are:

Default IP Address: 192.168.223.100
Default IP mask: 255.255.255.0
Default gateway: 192.168.223.254
Default Password: " admin "

1.2.2 Terminal mode default setting are: baud rate: 115,200, attribute: 8, None, 1, None
Terminal mode operation: Default Password: " admin "

Once terminal is connected, the basic operation rule are shown below

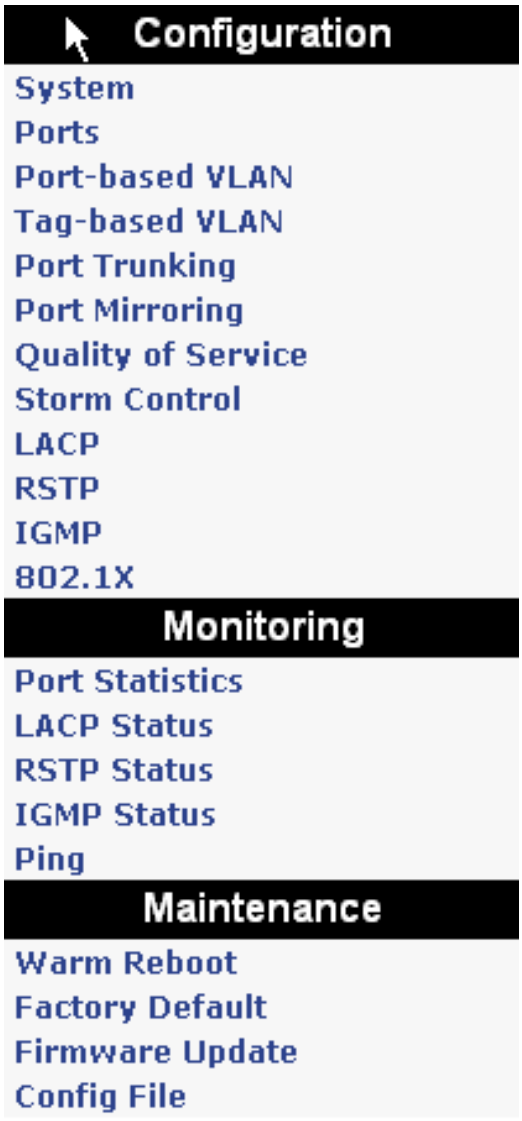
Press " ? " to find root operation page, then choose command by typing little alphabets

After enter command page, Press " ? " to find command parameters and format, further more, type " command ? " to get explanation.

Type " up " or " / " to go back to previous page

2.0 Web management

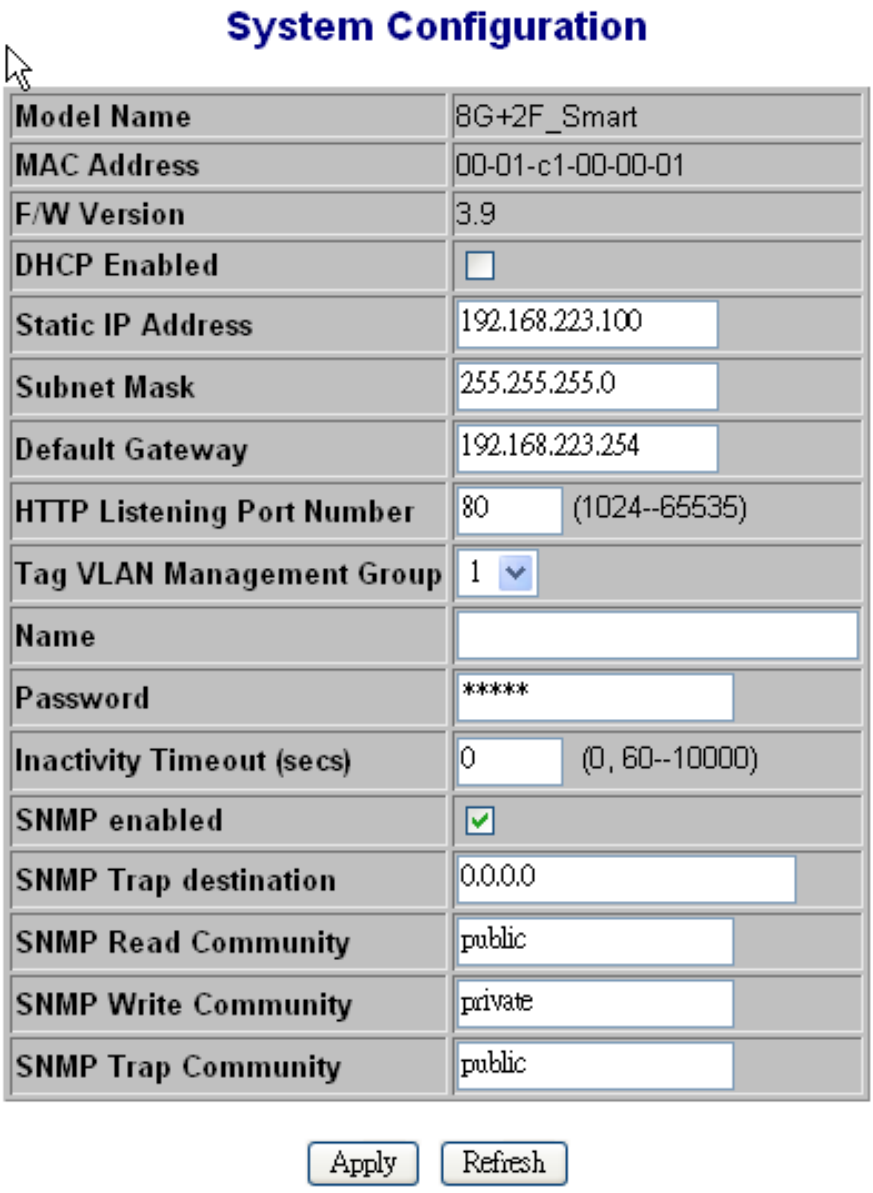
After login is successfully validated, the switch's home page will show up. The left part on the page provides the *function menus*, while the right part provides the individual configuration value or system parameters value. Function manuals are divided into three categories, they are **Configuration, Monitoring and Maintenance,** all functions are shown briefly below



2.1 Configurations

2.1.1.1 System information

The system diagram shows general common system information, they are H/W, F/W version, MAC address, IP address, subnet mask, IP gateway, default VLAN value of management port, name, password, timeout value, and SNMP communities…etc. Once user finish the setting, he must press the " Apply " button to execute all his setting, and whenever he needs, he may press the " Refresh " button to get updated status of system information.



2.1.1.2 DHCP

The default DHCP is off, so Default IP or user defined IP is used when this machine is turning-ON, but if this switch needs an IP assigned from DHCP server, user may click the square field and then press " Apply " to get an IP which will be assigned by DCHP server ". User must be aware that if he enable DHCP from web page, and if the DHCP server is working, then after enable DHCP, he will lose contact of web page, because the IP address has been changed. **At this moment, go through terminal mode and check configuration of IP, then get Dynamic IP to return web page.**

2.1.1.3 relocate HTTP port number

The default port number of **HTTP command** is 80, but unauthorized user may intrude this switch if he knows the IP of this switch, network manager may relocate this port number to other value, from 1024 to 65535, the same idea as above, once network manager change the value of HTTP's port number, he will lost contact and he must regain web page by command modified as below:

http://192.168.223.100:port_value

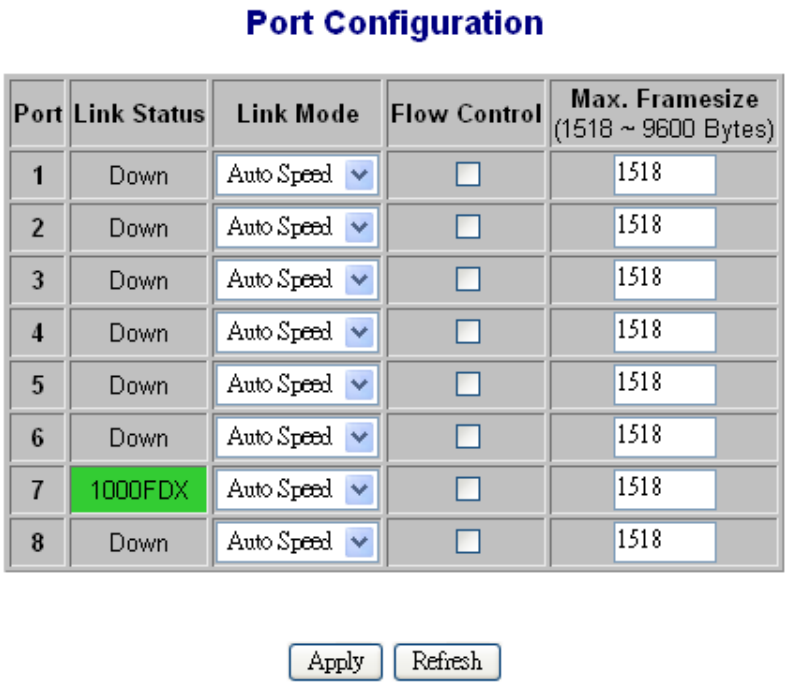
2.1.1.4 Tag VLAN management group (CPU port)

At first time you turn on this device, all ports belong to default VLAN ID group (VID=1), so they can communicate to each other, and hence any port can be used as web management port to talk with CPU port inside, but, for example, assume user uses port 1 as web management port, then user create VLAN ID=10 on port 7,8 and create another VLAN ID = 20 on port 5,6, now 3 VLAN groups will be shown on VALN group table after he press " Apply " button. If VLAN 10 and VLAN ID 20 must be isolated, then user must delete member port 5,6,7,8 in default VLAN group(VID = 1). Be aware that CPU port is still remain on VID=1 group now, user can only perform web management through one of 4 ports, that is port 1,2,3,4, **but if user want to perform web management from other port in existing different VLAN group, for example port 8 in VID =10, then after creating new VLAN groups, he must go to system configuration page, and select Tag VLAN Management Group to 10 by pressing " Apply " command,** then move RJ-45 (web management port) from port 1 to port 8, then user can perform web management from new RJ-45 port again. But if user forget what group that CPU belongs to, there are two ways to solve this condition below.

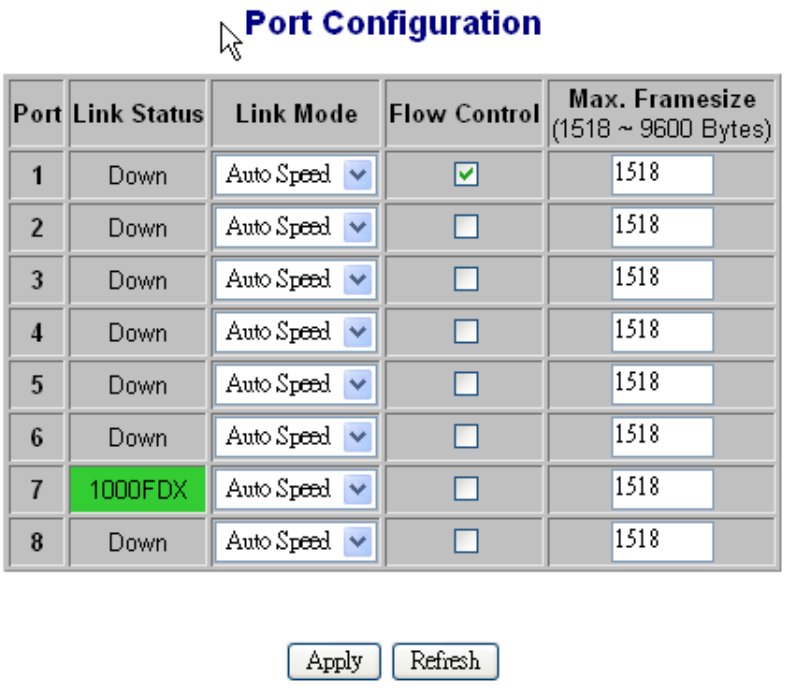
(1) Through console port, check configuration of IP if he gets password, or
(2) Press **"Reset"** button **few seconds**, let system return to default settings, that is,
---- >> IP address=192.168.223.100; … VID=1, all settings return to factory default

2.1.2 Ports

Port status page always shows current port status of all 8 ports. User can set link mode, enable or disable flow control and jumbo frame, however, be noticed that the jumbo frame is global setting, it can't be set on individual port but on all ports at a time. A default diagram is shown below,

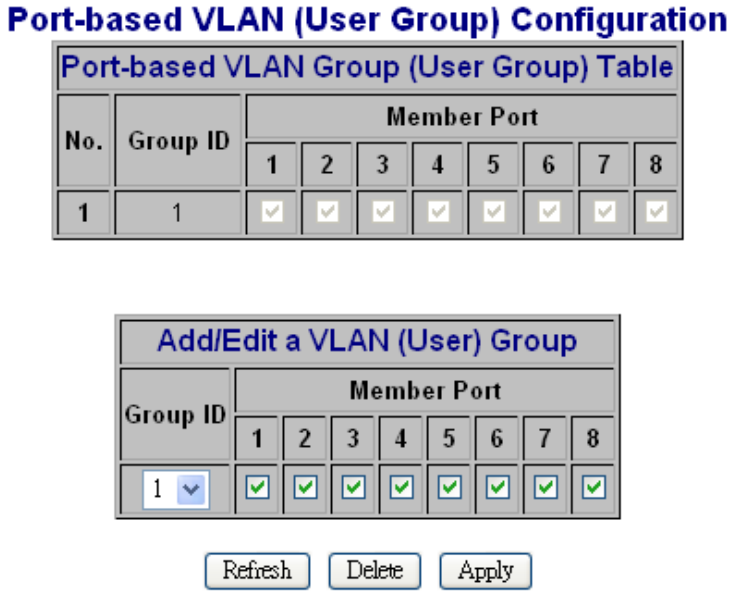


Choose and click the ports you want to set, for example, choose port 1, and set port 1 Flow Control enable, then press "Apply", after execution, diagram will shown below

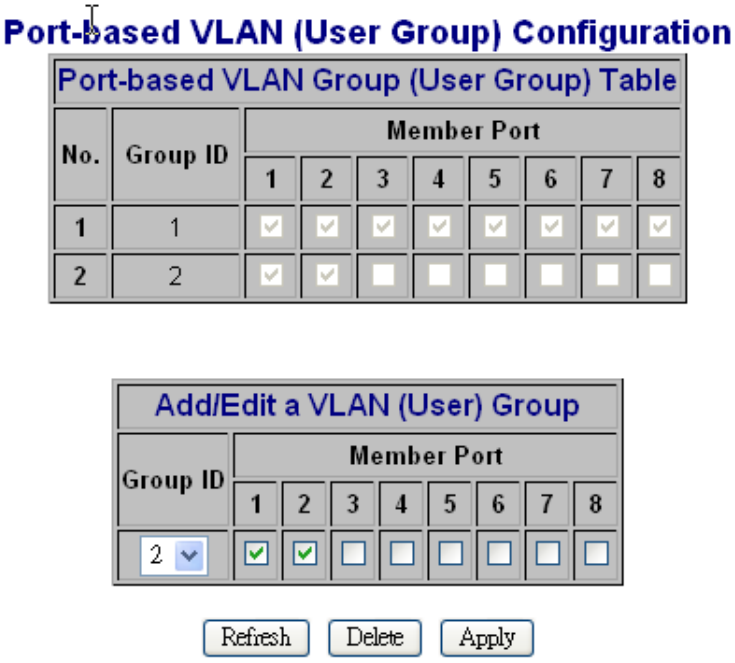


2.1.3 Port-based VLAN

Port-based VLAN is a kind of VLAN which is a group of ports marked as a kind by group ID, different VLAN (different ID) can't communicate to each other. Before the setting, user must be aware of that there is a default Port-based VLAN, his group ID is 1, so, if user wants to set another new port-based VLAN, better set another group ID rather than 1. After press " Apply " button, the screen will show a updated VLAN Group table no matter user add a new group or delete a VALN group. The important thing is that port-based VLAN is valid only within same device, it will never be valid cross the devices. A default diagram is shown below.



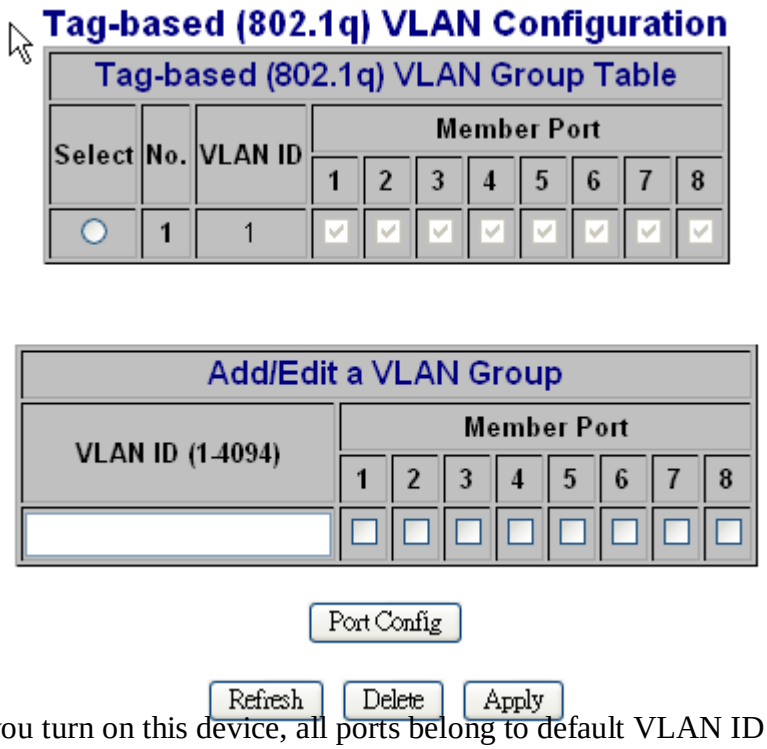
Choose and click the ports you want to group, for example, choose port 1, port 2 and set their group ID 2, then press "Apply", after execution, diagram will shown below



2.1.4 Tag-based VLAN

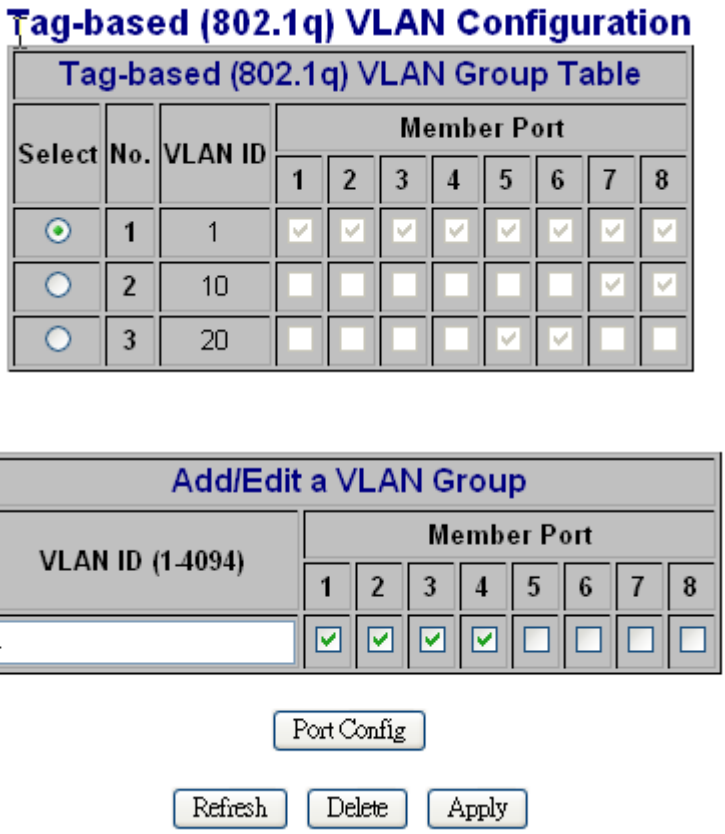
Tag-based VLAN is another kind of VLAN which is a group of ports marked as same kind by assigning a tag-value on each port, same as port-based VLAN, different VLAN (different ID) can't communicate to each other, and before the setting, there is a default tag-based VLAN, which ID is 1 (VLAN ID=1), so, if user wants to create another new tag-based VLAN, better set another VLAN ID rather than 1 (tag-based VALN ID ranged from 1 ~ 4094). After press " Apply " button, the screen will show a new tag-based VLAN Group table, on the contrary, a tag-VLAN will be vanished if user delete a VLAN group. **Two important things must be emphasized here,** one is that tag-based VLAN members are valid not only within same device, but also cross the devices as long as they are with same VLAN ID; the other important thing is user must keep in mind that the **VLAN ID of CPU port must be one of the VLAN group if user wants to manage through one of the ports of that VLAN group,** otherwise, if there is no port with same VLAN ID as CPU port, the web management, in-band control, will be failed because different VLAN (different ID) can't communicate to each other.

A default diagram is shown below.



The first time you turn on this device, all ports belong to default VLAN ID group (VID=1), so they can communicate with each other, and hence any port can be used as web management port to talk with CPU port inside, but, for example, assume user uses port 1 as web management port, then user create VLAN ID=10 on port 7,8 and create another VLAN ID = 20 on port 5,6, now 3 VLAN groups will be shown on VLAN group table after he press " Apply " button.

If VLAN 10 and VLAN ID 20 must be isolated, then user must delete member port 5,6,7,8 in default VLAN group(VID = 1). See below



Be aware that CPU port is still remaining on VID=1 group now, user can only perform web management through one of 4 ports, that is port 1,2,3,4, **but if user want to perform web management from other port existing in different VLAN group, for example port 8 in VID =10, then after creating new VLAN groups, he must go to System Configuration page, and select Tag VLAN Management Group to 10 by pressing " Apply " command,** then move RJ-45 (web management port) from port 1 to port 8, then user can perform web management from new RJ-45 port again. But if user forget what group that CPU belongs to, there are two ways to solve this condition below.

(1) Through console port, check Configuration of IP if he gets password, or
(2) Press **"Reset"** button **few seconds**, let system return to default settings, that is,
---- >> IP address=192.168.223.100; … VID=1, all settings return to factory default

After assign a tag VLAN, there are some attributes parameters must be assigned for some tag-VLAN application, here below are explanation when entering the " Port Config ", they are:

1. VLAN Aware mode:

Enable – When Tag-VALN function is applied on this port, user may enable VLAN Aware associated with this port, then ingress frames and egress frames will be handled according to the following parameters' setting.

Disable – default state, this means, switch doesn't do VLAN tag stripping and insertion.

2. Ingress filtering:

Enable - Check ingress frame VLAN ID. Ingress frame will be dropped if this frame's VID is not the same as the VID of the ingress port which belongs to a member of a VLAN group

Disable – the Ingress frame will be flood if VID is not the same

3. Accept Packet Type:

ALL - Accept all ingress frames

Tagged only - Only accept ingress frames with VLAN tag

4. **Port VID**:

Set **Port VID** = value (1 ~ 4096), then an untagged ingress frames will bear this value a its VID, usually this port is connected to un-tag device (legacy device), then this frame become a tagged frame, hence, it can be handled inside the switch as a member of same VID group.

Set "None" for those tagged frames, usually this port is now connected to a tag-device

5. **Egress Tag enable**

When Egress Tag is enabled, then, the tag will be added into egress frames and then sent out to the device that support tagged-VLAN, when this is disabled, tag will not be added into egress frame and then sent to device that does not support tagged-VALN.

Tag VLAN Per Port Configuration

Port	VLAN aware Enabled	Ingress Filtering Enabled	Acceptable Packet Type	Port VID	Egress Tagging Enabled
1	☐	☐	◉ All ○ Tagged Only	1	☐
2	☐	☐	◉ All ○ Tagged Only	1	☐
3	☐	☐	◉ All ○ Tagged Only	1	☐
4	☐	☐	◉ All ○ Tagged Only	1	☐
5	☐	☐	◉ All ○ Tagged Only	1	☐
6	☐	☐	◉ All ○ Tagged Only	1	☐
7	☐	☐	◉ All ○ Tagged Only	1	☐
8	☐	☐	◉ All ○ Tagged Only	1	☐

Apply Back

2.1.5 Port Trunking

A default diagram is shown below, and up to 4 groups are provided

Aggregation/Trunking Configuration

Group\Port	1	2	3	4	5	6	7	8
Normal	◉	◉	◉	◉	◉	◉	◉	◉
Group 1	○	○	○	○	○	○	○	○
Group 2								
Group 3								
Group 4								

Apply Refresh

Choose and click the trunk ports you want to group, for example, choose port 1, port 2 into group 1, then press "Apply", after execution, diagram will shown below

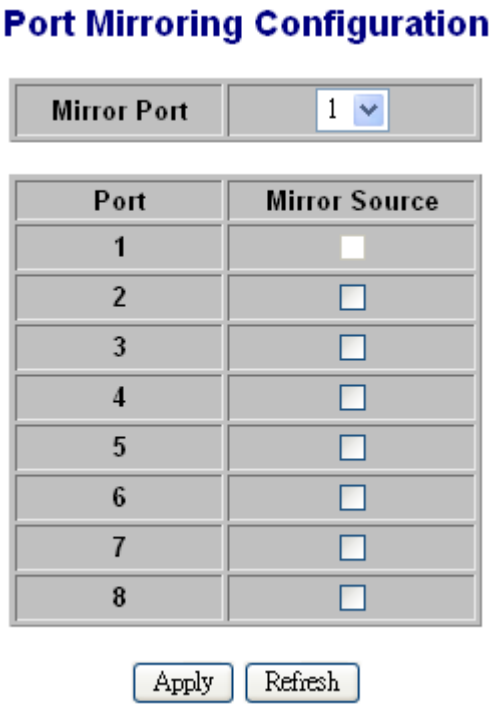
Aggregation/Trunking Configuration

Group\Port	1	2	3	4	5	6	7	8
Normal	○	○	◉	◉	◉	◉	◉	◉
Group 1	◉	◉	○	○	○	○	○	○
Group 2	○	○	○	○	○	○	○	○
Group 3								
Group 4								

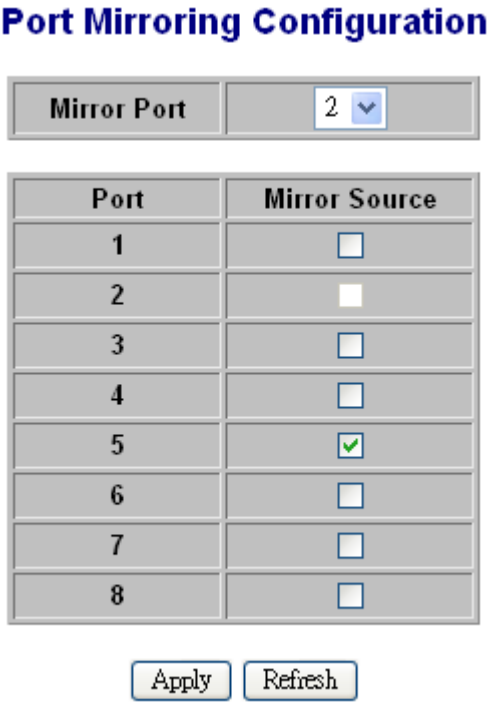
Apply Refresh

2.1.6 Port Mirroring

A default diagram is shown below,



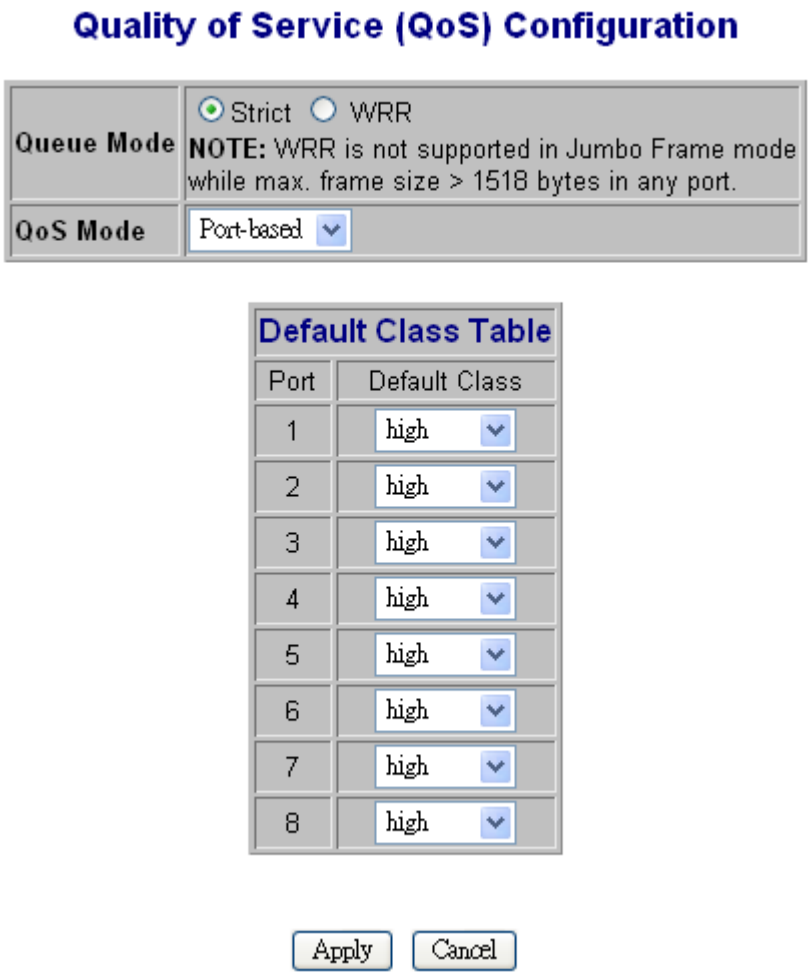
Choose and click the ports you want to monitor, for example, choose port 2 is mirror port And the mirror source is port 5. then press "Apply", after execution, diagram will shown below



2.1.7 Quality of Service

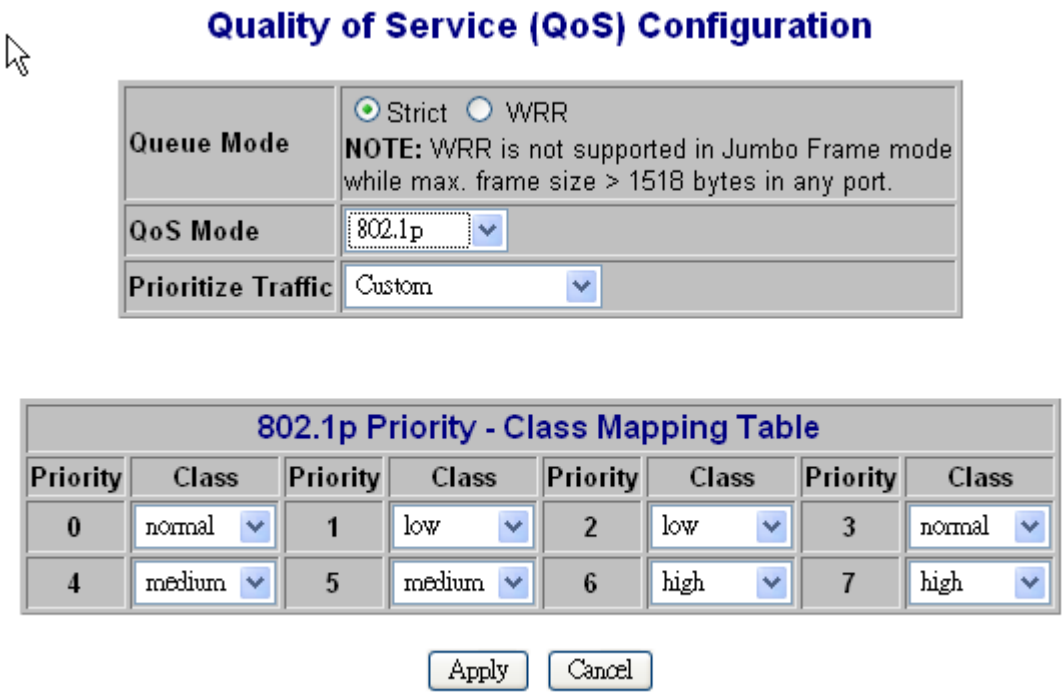
There are 4 class priority can be set for each port: Low, Normal, Medium and High, because there are 8 priority levels (0 ~ 7) for each port, so 8 priorities map into 4 class must be done in this QoS control.

There are 3 QoS Mode can be chosen: Port-based, 802.1P and DSCP. The frames sending not only per priority setting but also per Queue Mode setting. **Strict Mode** means highest priority setting gets first service to send frames, the lower priority frames must wait until all other higher priority frames are sent (serviced), then it gets service. **WRR Mode** means different priority are with different weighting to get service, that is, within a time period, the service times (chance) are a ratio among these 4 classes, user may choose one of preset setting from the manual. A default diagram with Strict Queue Mode is shown below



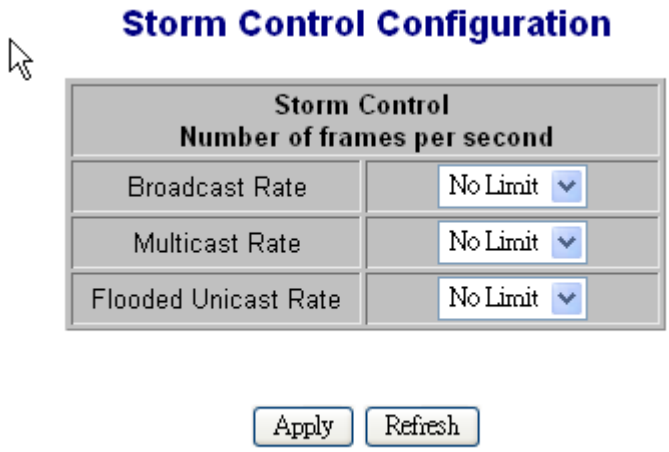
Choose the port-based priority level for each port you want to set, then ports will get priority service as setting, for example, Under Strict Mode, Port 5,6,7,8 are set " low ", port 1,2,3,4 are set as high, medium, normal and low. Then, after " Apply ", usually port 1 will get service at most of time and even all of the time.

When user choose the 802.1P priority, this means frames are with VLAN Tag inside the switch, the priority in the Tagged frame (2 bytes Tag in total) must be set by application program. But 8 priority levels map into 4 class also must be done same as explained in previous paragraph.

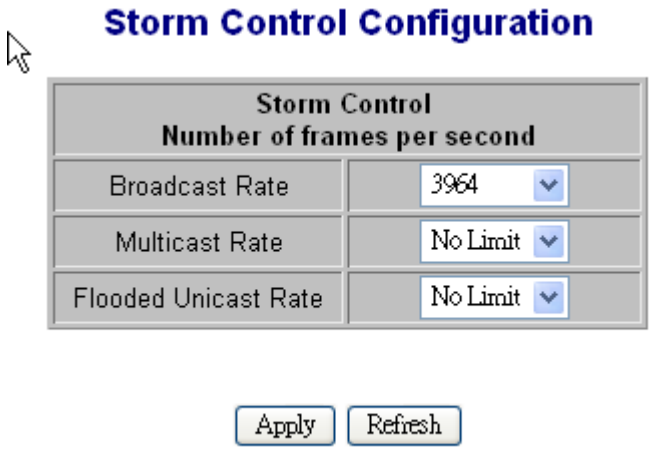


2.1.8 Storm Control

A default diagram is shown below,

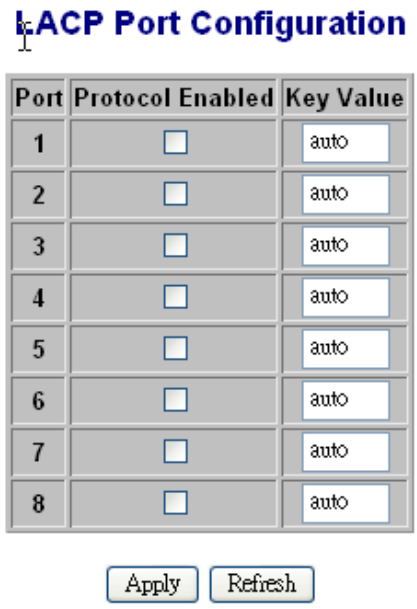


Choose and click type of storm you want to control, for example, choose Broadcast storm with 3,964 frames per second as upper limit, once the Broadcast frame rate higher than 3,964 frame per second, this port will be disabled. Press "Apply", after execution, diagram will be shown below



2.1.9 LACP

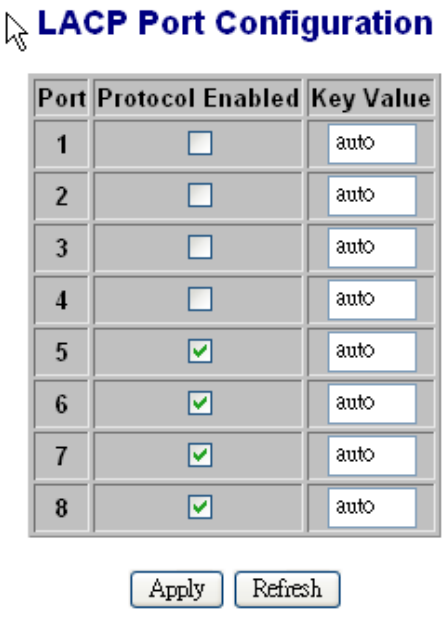
Different from the static port trunking, LACP provides another way to dynamically aggregate port to a group (trunk) according to IEEE 802.3ad. Once the protocol is enabled, the ports to be trunked by LACP will be executed automatically after press " apply " A default diagram is shown below,



Two parameters need to be set per port basis in this webpage:

- **Protocol Enabled** – to enable/disable LACP protocol for a port.
- **Key Value** – a number (1~255) to identify the LACP group for a port. All member ports in a LACP group have the same key values. Key number will be automatically generated if "auto" value is set

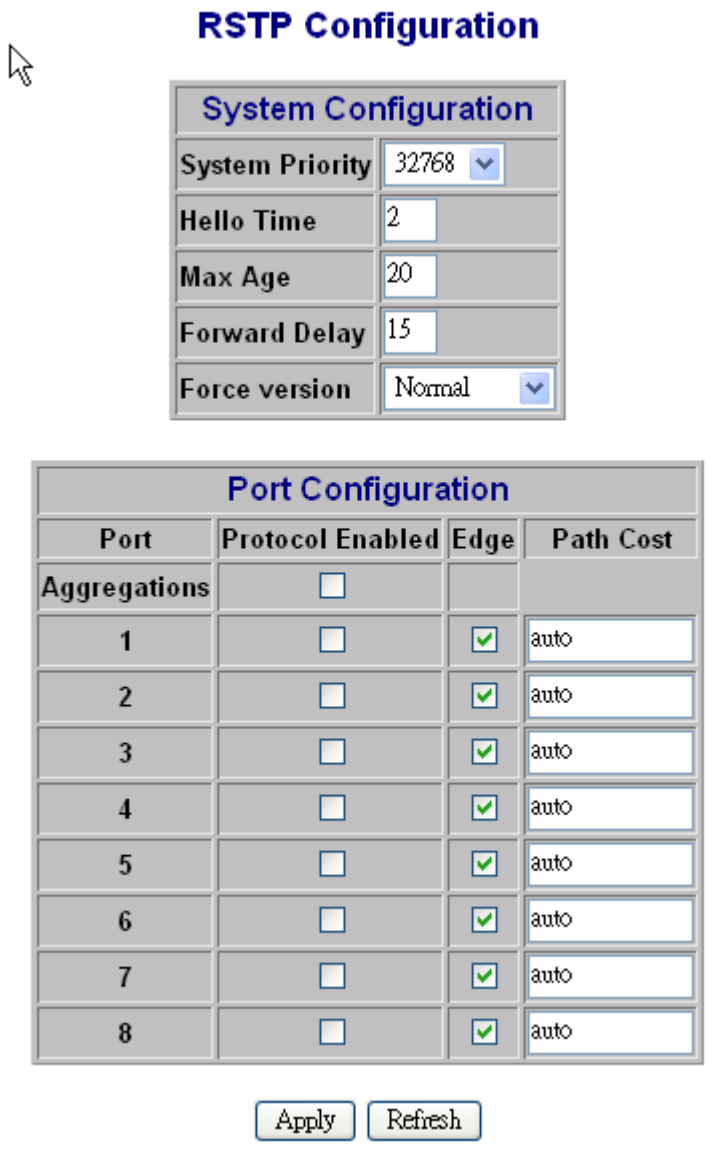
Choose and click the trunk ports you want to group. For example, select port 5, 6, 7 and port 8 to group into a LACP group with key value "auto" for all ports, then press " Apply" to activate the setting. The figure is shown below



2.1.10 RSTP

The Spanning-Tree Protocol (STP) is IEEE 802.1d standardized method for avoiding loops in switched networks. Enable STP to ensure that only one path at a time is active between any two nodes on the network.

The Rapid-Spanning-Tree-Protocol (RSTP) is a more advanced protocol than STP according to IEEE 802.1w standard. RSTP can shorten spanning tree convergent time while network topology is changed. A default diagram is shown below,



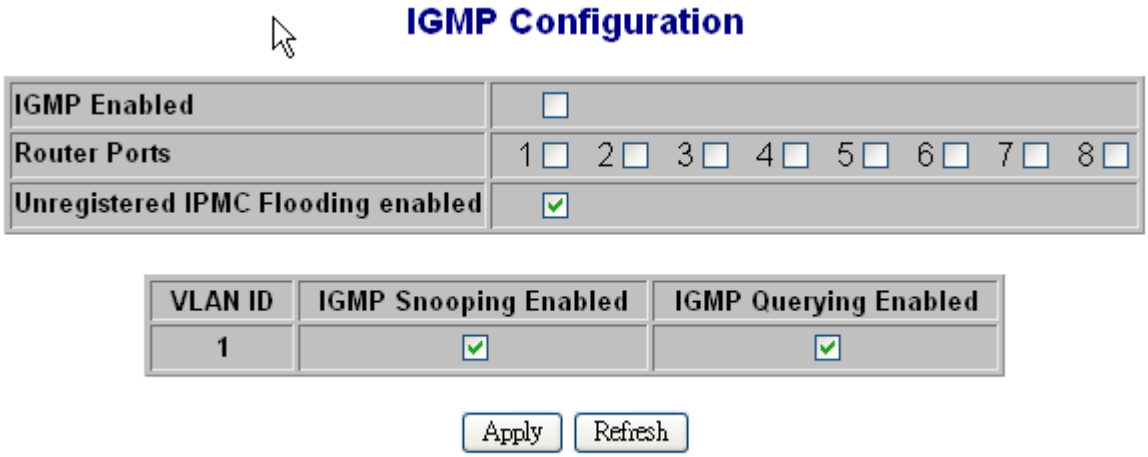
Use the following parameters in the webpage to configure RSTP function:

- **System Configuration**
  - **System Priority** – A value to identify the root bridge. The bridge with lowest value has the highest priority and is selected as the root. 16 numbers are provided in this field from 0 to 61140 in increments of 4096.
  - **Hello Time** -- the number of seconds among the transmission of Spanning-Tree Protocol configuration messages. Enter a number 1 through 10. (default is 2)
  - **Max Age** – the number of second bridge waits without receiving Spanning-Tree Protocol configuration messages before attempting a reconfiguration. Enter a number 6 through 40. (default is 20)
  - **Forward Delay --** the number of seconds a port waits before changing from its Spanning-Tree Protocol learning and listening states to the forwarding state. Enter a number 4 through 30. (default is 15)
  - **Force Version** – normal: use RSTP; compatible: compatible with old STP protocol

- **Port Configuration**
  - **Aggregations** – Enable/disable the RSTP protocol on aggregation links
  - **Protocol Enabled** – Enable/disable the RSTP protocol per port basis
  - **Edge** – Enable/disable to expect a port to be an edge port (an end station) or a link to another STP device
  - **Path Cost** – A value on a port that switch uses to determine which port are the forwarding ports. The lowest number is forwarding ports. The value can be set from 1 to 200000000 or "auto" to be automatically generated.

2.1.11 IGMP

The Internet Group Management Protocol (IGMP) is an internal protocol of the Internet Protocol (IP) suite. IGMP can manage the multicast traffic if the members (switches, router or other network devices) of group support IGMP. This switch provides IGMP snooping feature to detect IGMP queries, report packets and manage the IP multicast traffic through the switch. This feature can limit the forwarding multicast frames only to those ports that are a member of multicast group. Only **IPv4** IGMP frames are recognized for this system.



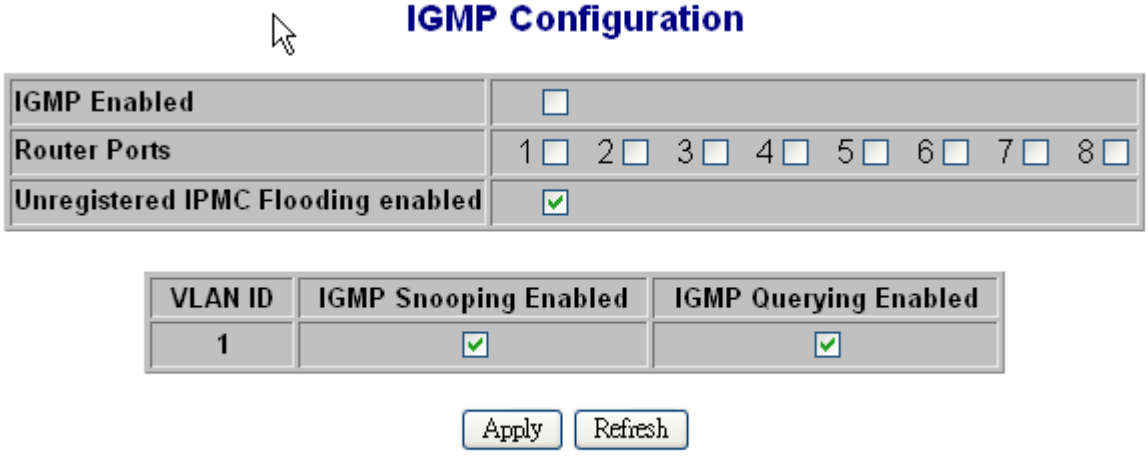
The following parameters are provided for configuring IGMP snooping for this system:

- **IGMP Enabled** – to globally enable/disable IGMP snooping function
- **Router Ports** – the port that is usually with source of multicast traffic stream
- **Unregistered IPMC Flooding Enabled** – to set forwarding option for unregistered (not joined) IP multicast traffic.
  Enabled: to flood frames to every port;
  Disable: to forward frames only to those IGMP member ports

Two options can be set for each existing group:

- **IGMP Snooping Enabled** – to enable/disable snooping IGMP frames
- **IGMP Querying Enabled** – to enable/disable sending IGMP querying frames, in one Ethernet subnet, there is only one Querier, and Querier is usually a router device

For example, video traffic comes from port 8 which is connected to a router, and port 3, 4, 5 are Connected to IGMP member, then the configuration may be set as below



2.1.12 802.1x

A default diagram is shown below, user must contact the manager of RADIUS server, and then get IP, UDP port number (usually fixed at 1812) and secret to operate 802.1X.

Admin Mode:

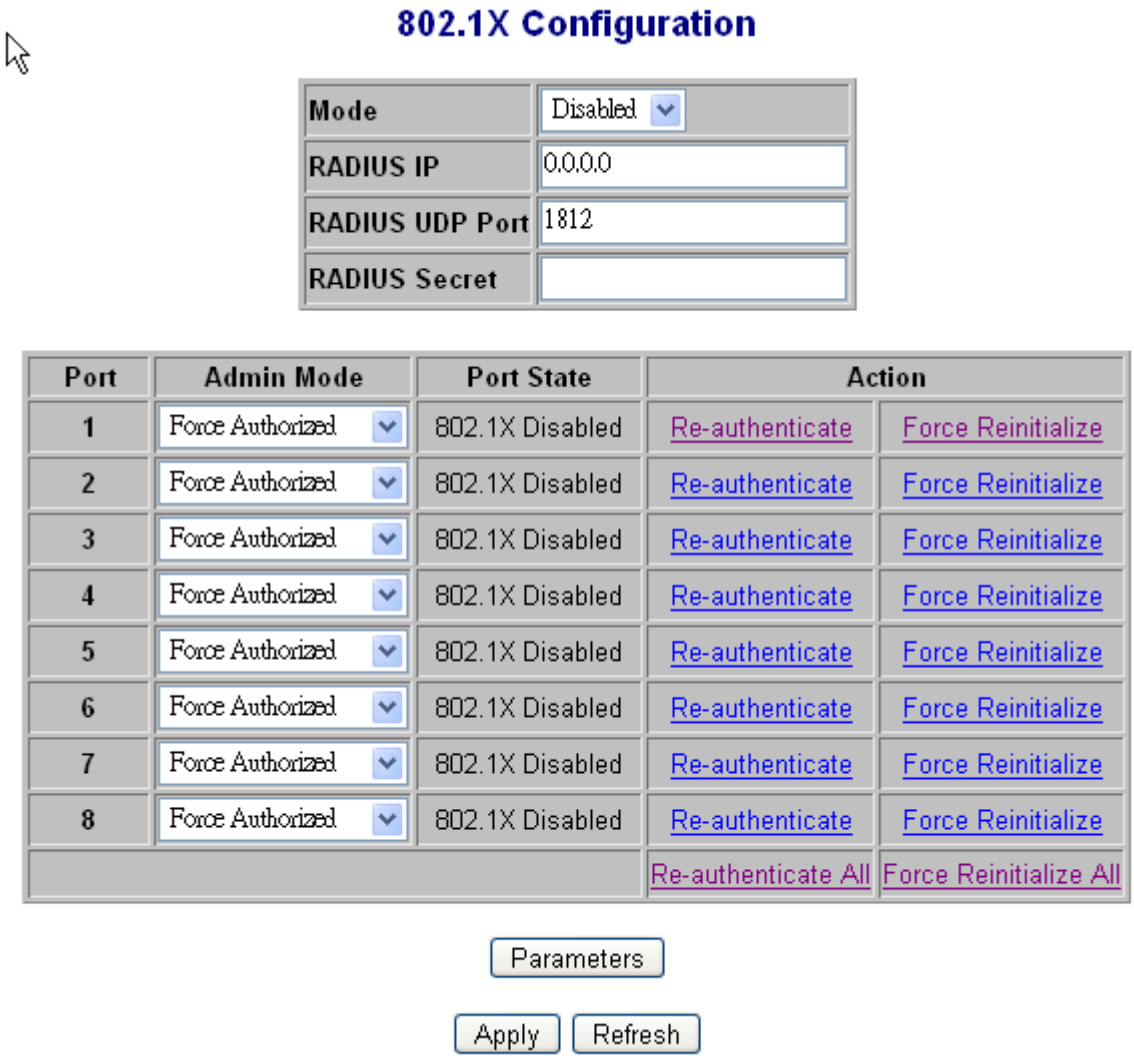
Auto: client will be authorized by authentication process
Force Authorized: client will be authorized anyway
Force Unauthorized: client won't be authorized anyway

Action: means execute command on single port or all ports when click

Re-authenticate: authorized again on that port
Force Reinitialize: force that port initialize
Statistic: see statistic frames

Parameters: Define time schedule on Re-authentication mode

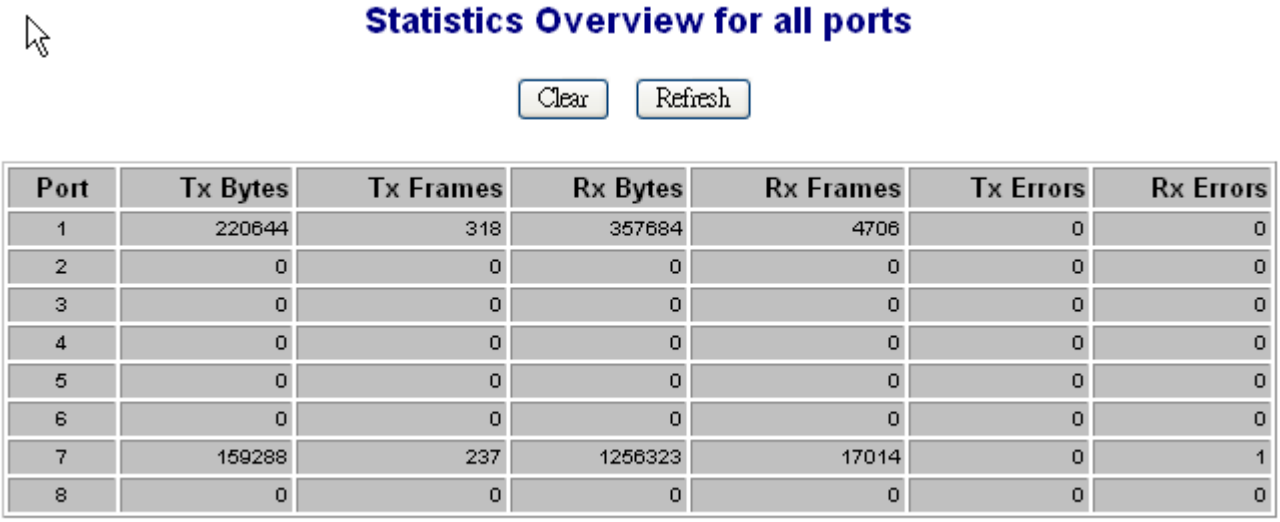
The default diagram as shown below:



2.2 Monitoring

2.2.1. Port Statistics

Choose and click command manual, after execution, diagram will shown below, user can clear counter or refresh as will



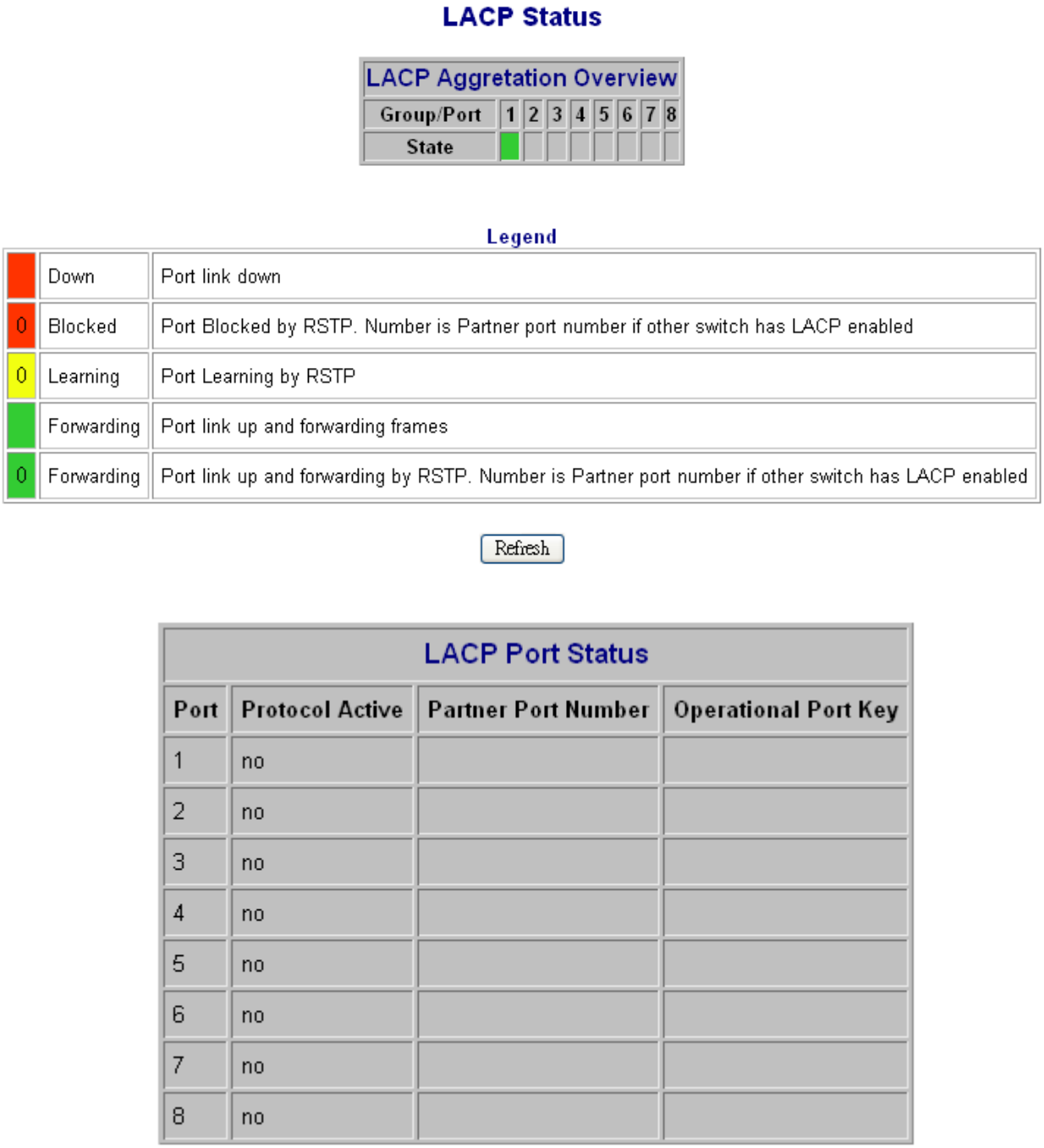
Statistics Overview for all ports

Clear Refresh

Port	Tx Bytes	Tx Frames	Rx Bytes	Rx Frames	Tx Errors	Rx Errors
1	220644	318	357684	4706	0	0
2	0	0	0	0	0	0
3	0	0	0	0	0	0
4	0	0	0	0	0	0
5	0	0	0	0	0	0
6	0	0	0	0	0	0
7	159288	237	1256323	17014	0	1
8	0	0	0	0	0	0

2.2.2 LACP Status

Choose and click command manual, after execution, diagram will shown like below, user can refresh at will.



LACP Status

LACP Aggretation Overview								
Group/Port	1	2	3	4	5	6	7	8
State								

Legend

	Down	Port link down
0	Blocked	Port Blocked by RSTP. Number is Partner port number if other switch has LACP enabled
0	Learning	Port Learning by RSTP
	Forwarding	Port link up and forwarding frames
0	Forwarding	Port link up and forwarding by RSTP. Number is Partner port number if other switch has LACP enabled

Refresh

LACP Port Status			
Port	Protocol Active	Partner Port Number	Operational Port Key
1	no		
2	no		
3	no		
4	no		
5	no		
6	no		
7	no		
8	no		

2.2.3 RSTP Status

Choose and click command manual, after execution, diagram will shown like below, user can refresh at will.

RSTP Status

RSTP VLAN Bridge Overview						
VLAN Id	Bridge Id	Hello Time	Max Age	Fwd Delay	Topology	Root Id
1	32769:00-01-c1-00-00-02	2	20	15	Steady	This switch is Root!

Refresh

RSTP Port Status						
Port/Group	Vlan Id	Path Cost	Edge Port	P2p Port	Protocol	Port State
Port 1						Non-STP
Port 2						Non-STP
Port 3						Non-STP
Port 4						Non-STP
Port 5						Non-STP
Port 6						Non-STP
Port 7						Non-STP
Port 8						Non-STP

2.2.4 IGMP Status

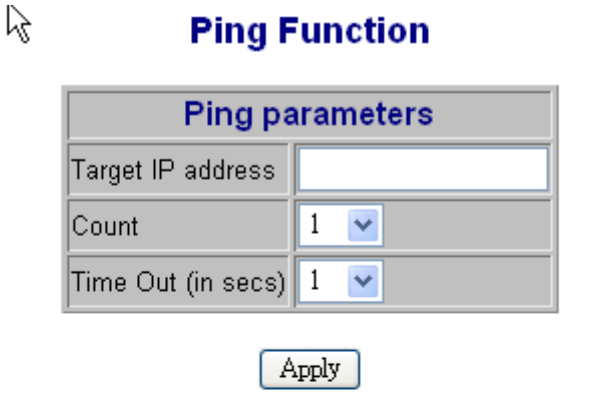
Choose and click IGMP status at command, after execution, diagram will be shown like below, user can refresh as will. There are IGMP v1, v2,v3 frames will be shown in the network, our switch only support IGMP V2, but it will handle some IGMP V3 frames. If this switch is Querier, it will show Querier state and Query frames it transmitted, if it is not Querier, it only show how many Querier frames it receives. Only one Querier in a network subnet, usually Querier is a router.

IGMP Status

VLAN ID	Querier	Queries transmitted	Queries received	v1 Reports	v2 Reports	v3 Reports	v2 Leaves
1	Disabled	0	0	0	0	0	0

Refresh

2.2.5 Ping



Ping Results	
Target IP address	0.0.0.0
Status	Test complete
Received replies	0
Request timeouts	0
Average Response Time (in ms)	0

Refresh

Fill up the IP address you want to ping, set Time Out time and Counts, for example, IP = 192.168.223.25441, count = 5, time pout = 5 sec, then press "Apply", then press "Refresh" after execution, diagram will shown below

Ping Results	
Target IP address	192.168.1.141
Status	Test complete
Received replies	5
Request timeouts	0
Average Response Time (in ms)	4

Refresh

2.3 Maintenance

2.3.1 Warm Reboot

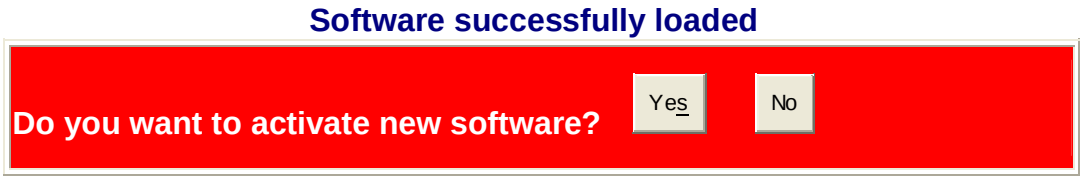
Choose and click command manual, diagram will shown like below, user can press Yes or No

2.3.2 Factory Default

Choose and click command manual, diagram will shown like below, user can press Yes or No

2.3.3 Firmware Update

Choose and click command manual, diagram will be shown, and then direct the location of the file that is to be updated, then press " upload ", if success, it will be shown below

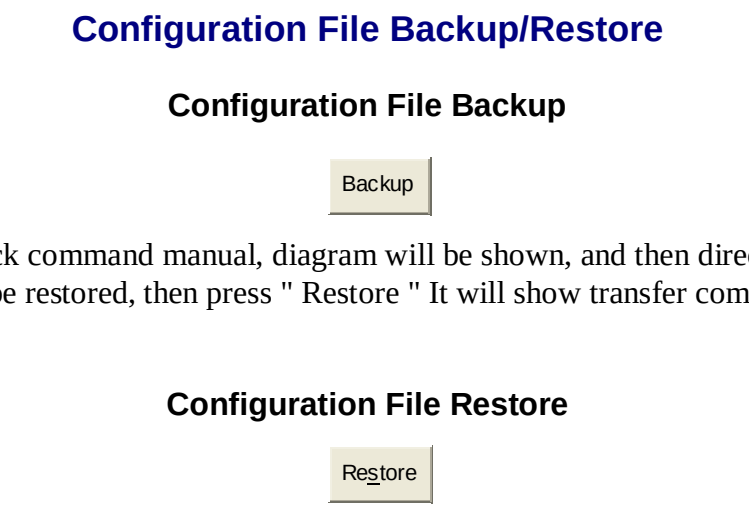


Press, "yes" then you get new code to execute, **however, after activate the new code,** then, 5 ~ 10 seconds later, press "**reset button**" **at front panel** so that the new default setting will be also updated, because different version of code is usually with different data structure of initial default setting

Note: Pressing and holding the reset button to perform a factory reset is very important in order to ensure further smooth operation on the switch after software upgrade.

2.3.4 Config File

Choose and click command manual, diagram will be shown, and then direct the location of the file that is to be backup, give a name, then press " Backup "



Choose and click command manual, diagram will be shown, and then direct the location of the file that to be restored, then press " Restore " It will show transfer completed if it success.

3.0 Terminal Mode Management

Terminal mode is easy to operate, it is useful when in-band Ethernet communication is malfunctioning, or user has to use CLI interface operation, or he wants to know some parameter setting, for example, before in-band management through Ethernet, user has to know the IP address, subnet mask, …etc, he may get this information by checking the configuration under IP command, he also may try to modify the IP address, CPU management group used in tag-VLAN configuration operation, or any other function through terminal mode. And most convenient, if user is used to configure the tag-VALN through terminal mode, he won't be interfered by the CPU management group issue, CPU is always being connected with him while he is configuring the VLAN.

User must set up the terminal parameters, such as Hyper terminal in Microsoft Window,

Select COM #: COM 1, COM 2, …then,
Set Baud rate to: 115,200, per second
Set Attribute to 8, None, 1, None (8 bit, No parity, 1 stop bit, No protocol in hardware)

Once terminal is connected, enter the password, the basic operation are shown, and then when press **" ? "** the **commands at top level** will be shown as below.

```
>?
Commands at top level:
System       - System commands
Console      - Console commands
Port         - Port commands
MAC          - MAC commands
VLAN         - 802.1q (Tag-based) VLAN commands
Aggr         - Aggregation commands
LACP         - IEEE 802.3ad Link Aggregation commands
RSTP         - IEEE 802.1w Rapid Spanning Tree commands
User Group   - User Group (Port-based VLAN) commands
QoS          - QoS commands
Mirror       - Mirror commands
IP           - IP commands
Dot1x        - Dot1x commands
IGMP         - IGMP Snooping commands
>
```

Key in " Command " and then key in " ? ", second level will be shown , for example

```
>vlan
VLAN>?
Commands at VLAN level:
VLAN Configuration [<portlist>]
VLAN Add <vidlist> [<portlist>]
VLAN Delete <vidlist>
VLAN Lookup <vidlist>
VLAN Aware [<portlist>] [enable|disable]
VLAN PVID [<portlist>] [<vid>|none]
VLAN Frame Type [<portlist>] [all|tagged]
VLAN Ingress Filtering [<portlist>] [enable|disable]
VLAN Egress Tagging [<portlist>] [enable/disable]
```

```
VLAN>conf
VLAN Configuration:
    Port  Aware    PVID  Ingress Filtering  Frame Type  Egress Tagging
     1:  disabled    1       disabled          All         disabled
     2:  disabled    1       disabled          All         disabled
     3:  disabled    1       disabled          All         disabled
     4:  disabled    1       disabled          All         disabled
     5:  disabled    1       disabled          All         disabled
     6:  disabled    1       disabled          All         disabled
     7:  disabled    1       disabled          All         disabled
     8:  disabled    1       disabled          All         disabled

    Entries in permanent table:
       1:  1,2,3,4,5,6,7,8
VLAN>
```

If user wants to check the IP related information, he may do as below

```
IP>conf
IP Configuration:
    dhcp: disabled
    Static Address: 192.168.223.100
    Subnet Mask: 255.255.255.0
    Gateway: 192.168.223.254
    VID: 1
    HTTP Port No.: 80
    Mode:  enabled
    tftp: disabled
IP>
```

All other function can be operate likewise.

Type " up " or " / " go back to previous page

CTC union

www.ctcu.com

T +886-2 2659-1021 F +886-2 2659-0237 E info@ctcu.com

ISO 9001 Quality System Certified CTC Union Technologies Co.,LTD.

All trademarks are the property of their repective owners. Technical information in this document is subject to change without notice.